Kasra Ahmadi

PhD Candidate
Lutz, FL, 33559
EB2–NIW Approved (U.S. Permanent Residency in Process)

ahmadi1@usf.edu
Scholar Profile
GitHub Profile
LinkedIn Profile

Summary

Ph.D. Candidate specializing in **Machine Learning Security** and **Fault Resistant** Post-Quantum Cryptography (PQC) Algorithms. First author of **6 peer-reviewed publications**, including a **Best Paper Award** at the IEEE S&P 2025 workshop. Experienced in designing secure AI systems, cloud-native ML platforms, and production-grade software engineering workflows. Strong background in RAG security, federated learning privacy, and hardware reliability for AI systems.

Education

•PhD in Computer Science — *Jan 2022 - May 2025*
University of South Florida, Tampa, US — CGPA: 3.93

•Master in Information Technology Engineering — *Sep 2018 - Aug 2020*
AmirKabir University of Technology, Tehran, Iran — GPA: 16.69/20

Work Experience

–Graduate Research Assistant — *Jan 2022 - Present*
University of South Florida — Tampa, FL, US

* Publish 6 peer-reviewed papers as first author in leading venues (IEEE TVLSI, IEEE TCAS, ACM TECS), including a **Best Paper Award** at an IEEE S&P workshop in **ML Security** and **Fault Detection**.
* Designed hardware reliability techniques to **secure deep neural network** inference against fault injection attacks.
* Built a human-in-the-loop privacy utility optimization framework for **federated learning** systems.
* Researching the security of Led research on **securing RAG pipelines** by designing evasion attacks that perturb vector embeddings and degrade model accuracy.
* Developed low overhead, algorithm-level error detection for NTT modules used in lattice-based post-quantum cryptography and elliptic curve cryptography.

–AI Engineer Intern — *May 2025 - Aug 2025*
TD SYNNEX — Clearwater, FL, US

* Designed scalable, cloud-native AI platforms using LLMs, RAG, and multi-agent orchestration.
* Integrated safety and security guardrails across the agentic workflow to ensure robust production deployment.

–Software Engineer Intern — *May 2024 - Aug 2024*
TransparencyWise (AgWise) — St.Petersburg, FL, US

* Led a technical team in architecting an event-driven pipeline using AWS Lambda, S3, and Glue.
* Built a recommender system for nutrient optimization capable of supporting up to 1 million users simultaneously.

–Machine Learning Engineer — *Jan 2018 - Apr 2020*
PaarLift — Tehran, Iran

* Built an end-to-end ML solution from IoT data collection to model training and deployment.
* Used ensemble learning, KNN, and deep neural networks to optimize elevator parking floor predictions.
* Reduced passenger wait time by 27 percent across deployments in more than 100 commercial buildings.

Technical Skills

Languages: C/C++, Python, Verilog, Typescript, Javascript
Machine Learning Frameworks: PyTorch, Tensorflow, Langchain, Scikit-learn, Pandas
Web Dev Tools: Nodejs, Flask, Git, Docker, Websocket, GraphQL
Soft Skills: Mentorship Problem Solving, Self-learning, Presentation, Adaptability, Scrum

Selected Publications

-Ahmadi, K, et al (2025), "An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Model." In 2025 IEEE Security and Privacy Workshops (SPW). **(Best paper award)**

-Ahmadi, K, et al (2025), "Efficient Algorithm Level Error Detection for Number-Theoretic Transform Assessed on FPGAs and ARM" ACM Trans. Embed. Comput. Syst.

Selected Projects

–PII 360
GitHub, Product link

* Developed an open-source Chrome Extension that identifies Personally Identifiable Information (PII) in images and PDFs using ONNX-based machine learning models, running entirely on the client's local machine.

Certifications

- **AWS Certified Solutions Architect - Associate**
- Deep Neural Networks with PyTorch (IBM)
- Attention Mechanisms and Transformer Models
- Fundamentals of LLMs (HuggingFace)
- LangChain for LLM Application Development
- ETL and Data Pipelines with Shell, Airflow and Kafka (IBM)
- Generative AI - Technical AI Advisor (Nvidia)
- Fine-tuning Language Models (HuggingFace)